REMARKS/ARGUMENTS

Applicants have received the Office action dated April 21, 2005, in which the Examiner: 1) rejected claims 13-20 under 35 U.S.C. § 112, 1st paragraph, as failing to comply with the enablement requirement; 2) rejected claims 8 and 21 under 35 U.S.C. § 112, 1st paragraph, for the limitations, "wherein the applications detect...a newly-issued key"; and 3) rejected claims 1-7 and 9-10 under 35 U.S.C. § 103(a) as being unpatentable over Van Oorschot (U.S. Pat. No. 6,317,829) in view of Eastlake (Internet Draft). Based on the arguments contained herein, Applicants respectfully request reconsideration and allowance of the pending claims.

I. § 112 REJECTIONS

The Examiner rejected claims 13-20 as failing to comply with 35 U.S.C. §112, first paragraph. Specifically, the Examiner asserts that "the Applicant added new claims, but the Examiner cannot find in the specification the claim limitations described" (see Office Action, page 2, item 3). Applicants disagree with the Examiner.

Claim 13 requires "the database comprises entries defining at least one user of a first group of users and at least two users of a second group of users." Support for the limitations of claim 13 are found, at least, on page 13, lines 9-10 of Applicants' specification. Based on the information provided in the specification "any person skilled in the art to which [the invention] pertains" would be able to "make and use the [invention]" of claim 13 as is required under 35 U.S.C. §112, first paragraph.

Claim 14 requires "the first key has a value that is based on a password associated with the first group of users." Also, claim 15 requires "the second key has a value that comprises a plurality of value shares and wherein each value share is based on a password associated with the second group of users." Support for the limitations of claims 14 and 15 is found, at least, on page 13, line 23 – page 15, line 17 of Applicants' specification. Based on the information provided in the specification "any person skilled in the art to which [the invention]

pertains" would be able to "make and use the [invention]" of claims 14 and 15 as is required under 35 U.S.C. §112, first paragraph.

Claim 16 requires "a value associated with at least one of the first key and the second key is changed when at least one event occurs, the at least one event selected from a group of events consisting of: a user of the first group of users being added; a user of the first group of users being deleted; a user of the second group of users being added; a user of the second group of users being deleted; an algorithm used by the system being changed; and the database being rewritten." Support for the limitations of claim 16 is found, at least, on page 17, lines 17 – 28. Based on the information provided in the specification "any person skilled in the art to which [the invention] pertains" would be able to "make and use the [invention]" of claim 16 as is required under 35 U.S.C. §112, first paragraph.

Claim 17 requires "the key repository is configured to provide access to the second key in response to receiving a threshold number of valid passwords, each password associated with a different user from the second group of users." Support for the limitations of claim 17 is found, at least, on page 29, lines 7 – 20. Based on the information provided in the specification "any person skilled in the art to which [the invention] pertains" would be able to "make and use the [invention]" of claim 17 as is required under 35 U.S.C. §112, first paragraph.

Claim 18 requires "the second key permits modification of at least one security parameter selected from the group consisting of: a threshold number of valid passwords required to access the second key; users assigned to the first group of users; users assigned to the second group of users; pre-authentication of an application to access at least one of the first key and the second key without user intervention; cryptographic algorithms used by the system; and pre-authentication of a program to act as an extension of the key repository." Support for the limitations of claim 18 is found, at least, on page 10, lines 6 – 25. Based on the information provided in the specification "any person skilled in the art to which [the invention] pertains" would be able to "make and use the [invention]" of claim 18 as is required under 35 U.S.C. §112, first paragraph.

Claim 19 requires "the first key is used to encrypt a public key of an encryption algorithm." Also, claim 20 requires "the public key is used to encrypt a value associated with the first key and values shares associated with the second key." Support for the limitations of claims 19 and 20 is found, at least, on page 14, lines 13 – 18. Based on the information provided in the specification "any person skilled in the art to which [the invention] pertains" would be able to "make and use the [invention]" of claims 19 and 20 as is required under 35 U.S.C. §112, first paragraph.

The Examiner also rejected claims 8 and 21 as failing to comply with 35 U.S.C. §112, first paragraph. Applicants have amended the specification to include the limitations found in claim 8 and 21. Support for the amendment to the specification is provided by original claim 8. Based on the information provided in the specification "any person skilled in the art to which [the invention] pertains" would be able to "make and use the [invention]" of claims 8 and 21 as is required under 35 U.S.C. §112, first paragraph.

II. § 103 REJECTIONS

Claim 1, in part, requires "a first cryptographic key [that] protects an integrity of secret information stored in a database." Claim 1 further requires "a second cryptographic key [that] protects access to the secret information stored in the database."

The Examiner asserts that Van Oorschot teaches Applicants' claimed "a first cryptographic key [that] protects an integrity of secret information stored in a database" and "a second cryptographic key [that] protects access to the secret information stored in the database" (see Office Action, page 3, item 7 and page 6, item 21). Applicants disagree with the Examiner for the following reasons.

First, the Examiner incorrectly equates Applicants' claimed "second cryptographic key" with a password taught in Van Oorschot (see Office Action, page 3, item 7). While a password may be used to create and recover a cryptographic key (*e.g.*, via a password-based public key encryption), a password is not a "cryptographic key" as required in claim 1. Even Van Oorschot teaches that a password is separate from a cryptographic key and that a password may be

used as part of a decryption private key request 123 (see col. 7, lines 30-50 and col. 8, lines 5-37).

Second, the Examiner incorrectly equates Applicants' claimed "first cryptographic key [that] protects an integrity of secret information" with a "decryption private key encryptor" taught in Van Oorschot (see Office Action, page 3, item 7). Specifically, Van Oorschot teaches that the decryption private key encryptor is included "to help prevent unauthorized acquisition of the secret decryption keys" (see col. 6, lines 33-36). Therefore, the decryption private key encryptor protects "acquisition" of secret information rather than "an integrity of secret information" as required of the "first cryptographic key" in claim 1. Applicants submit that "an integrity of secret information" and "access to the secret information" are two separate limitations.

The Examiner appears to be distilling Applicants' claimed invention down to a "gist" or "thrust," in violation of the requirement to consider the claimed invention as a whole (see MPEP 2142.02). Van Oorschot simply teaches that either passwords or an encryption private key encryptor can be used to control access (or acquisition) of data. In contrast, claim 1 requires "a first cryptographic key [that] protects an integrity of secret information stored in a database" and "a second cryptographic key [that] protects access to the secret information stored in the database." None of the references cited by the Examiner, nor combinations of the references, teach or suggest the above limitations. For at least these reasons, Applicants submit that claim 1 and all claims that depend from claim 1 are allowable.

Claim 11, in part, requires "a first key [that] protects an integrity of secret information stored in a database." Claim 11 further requires "a second key [that] protects access to the secret information stored in the database."

As previously described, Van Oorschot simply teaches that either passwords or an encryption private key encryptor can be used to control access (or acquisition) of data. However, Van Oorschot does not teach or suggest "a first key [that] protects an integrity of secret information stored in a database" and "a second key [that] protects access to the secret information stored in the database"

as required in claim 11. None of the references cited by the Examiner, nor combinations of the references, teach or suggest the above limitations. For at least these reasons, Applicants submit that claim 11 and all claims that depend from claim 11 are allowable.

Amended claim 21, in part, requires "a first cryptographic key [that] protects an integrity of secret information stored in a database" and "a second cryptographic key [that] protects access to the secret information stored in the database." Claim 21 further requires that "the applications detect a missing key, and check with the Key Repository for that key and, if the missing key has been reissued, the applications receive a newly-issued key."

As previously described, Van Oorschot teaches that either passwords or an encryption private key encryptor can be used to control access (or acquisition) of data, but does not teach or suggest "a first cryptographic key [that] protects an integrity of secret information stored in a database" and "a second cryptographic key [that] protects access to the secret information stored in the database" as required in claim 21. None of the references cited by the Examiner, nor combinations of the references, teach or suggest the above limitations. Also, the Examiner previously suggested that claim 21 is allowable over the cited art based on the limitation "the applications detect a missing key, and check with the Key Repository for that key and, if the missing key has been reissued, the applications receive a newly-issued key." For at least these reasons, Applicants submit that claim 21 is allowable.

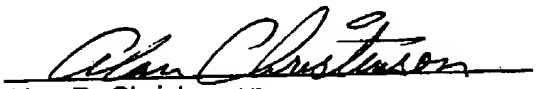
III. CONCLUSIONS

In the course of the foregoing discussions, Applicants may have at times referred to claim limitations in shorthand fashion, or may have focused on a particular claim element. This discussion should not be interpreted to mean that the other limitations can be ignored or dismissed. The claims must be viewed as a whole, and each limitation of the claims must be considered when determining the patentability of the claims. Moreover, it should be understood that there may be other distinctions between the claims and the cited art which have yet to be raised, but which may be raised in the future.

Appl. No. 09/736,717
Amdt. dated July 8, 2005
Reply to Office action of April 21, 2005

Applicants respectfully request reconsideration and that a timely Notice of Allowance be issued in this case. It is believed that no extensions of time or fees are required, beyond those that may otherwise be provided for in documents accompanying this paper. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required (including fees for net addition of claims) are hereby authorized to be charged to Hewlett-Packard Development Company's Deposit Account No. 08-2025.

Respectfully submitted,



Alan D. Christenson
PTO Reg. No. 54,036
CONLEY ROSE, P.C.
(713) 238-8000 (Phone)
(713) 238-8008 (Fax)
AGENT FOR APPLICANTS

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
Legal Dept., M/S 35
P.O. Box 272400
Fort Collins, CO 80527-2400